Safe and Secure Federal Websites Act: Section-by-Section Explanation

SECTION 1. SHORT TITLE.

This Act may be cited as the ``Safe and Secure Federal Websites Act of 2013".

Catchy title.

SEC. 2. ENSURING FUNCTIONALITY AND SECURITY OF NEW FEDERAL WEBSITES THAT COLLECT PERSONALLY IDENTIFIABLE INFORMATION.

(a) Certification Requirement.--

(1) In general.--Except as otherwise provided under this subsection, an agency may not deploy or make available to the public a new Federal PII website until the date on which a certification under subsection (b)(2) is submitted to Congress that the website is fully functional and secure.

Requires that all new federal websites that collect personally identifiable information (PII) be certified secure, subject to the rules and definitions that follow.

(2) Transition.--In the case of a new Federal PII website that is operational on the date of the enactment of this Act, paragraph (1) shall not apply until the end of the 30-day period beginning on such date of enactment. If the certification under subsection (b)(2) for such website has not been submitted to Congress before the end of such period, the head of the responsible agency shall render the website inaccessible to the public until such certification is submitted to Congress.

Allows 30 days to clean up the ObamaCare website before it is taken off-line. (There is no way to fix the site within 30 days, which only underscores the severity of the security failures.)

(3) Exception for beta website with explicit permission.--Paragraph (1) shall not apply to a website (or portion thereof) that is designed for testing and development purposes, if the following conditions are met:

(A) A member of the public may access PII-related portions of the website only after executing an agreement that acknowledges the risks involved.

(B) No agency compelled, enjoined, or otherwise provided incentives for such a member to access the website for such purposes.

Exception for voluntary beta testing.

(4) Construction.--Nothing in this section shall be construed as applying to a website that is operated entirely by an entity (such as a State or locality) that is independent of the Federal Government, regardless of the receipt of funding in support of such website from the Federal Government.

Clarifying that this does not apply to state exchange websites, whose sites should be governed by state law.

(b) Process for Study and Certification of Functionality and Security of New Federal PII Websites.--

(1) GAO study and report.--

(A) Study.--

(i) Current websites.--Not later than 30 days after the date of the enactment of this Act, the Comptroller General of the United States shall conduct a study of each new Federal PII website that is operational as of such date of enactment to determine whether such website is fully functional and secure.

(ii) Future websites.--Not later than 30 days after the date on which an advance notification is received under paragraph (3) for a new Federal PII website that is not operational as of such date of enactment, the Comptroller General shall conduct a study of such website to determine whether such website is fully functional and secure.

Requires the GAO conduct a study of the new federal website. Based upon subsequent input, it may be advisable to find an agency with better resources to do so, as GAO's team is quite small.

(B) Report to appropriate congressional committees.--Upon the completion of a study of a website under subparagraph (A) or (C), the Comptroller General shall submit to the appropriate committees of Congress and the Chief Information Officer for the responsible agency a report on the results of the study. Such report shall include a determination of whether the website is fully functional and secure.

(C) Followup studies and report.--If, based on the results of the most recent study under subparagraph (A) or this subparagraph, the Comptroller General determines that the website is not fully functional or

not secure, the Comptroller General shall conduct an additional study (and submit a report described in subparagraph (B) on the results of such study) until the Comptroller General determines that the website is determined to be fully functional and secure.

Because of constitutional issues with having GAO, a legislative agency, make binding determinations, GAO simply conducts the study (as many times as necessary) and reports the results to the agency and to Congress.

(2) Certification by CIO of responsible agency.--Upon the submission of a report under paragraph (1) that determines that a website operated by a responsible agency is fully functional and secure, the Chief Information Officer for such agency shall submit to Congress a certification of the results of such report and a certification as to whether the website is fully functional and secure.

The CIO certifies the website is good to go, and if the CIO ignores the GAO recommendation Congress will know.

(3) Advance notification for operation of future websites.--Each agency that intends to operate a new Federal PII website on or after the date of the enactment of this Act shall notify the Comptroller General of such intention and provide to the Comptroller General, in advance of the website becoming operational, such information as the Comptroller General may require to conduct a study and perform an evaluation under this subsection.

GAO is notified when a study will be needed and given necessary information.

(c) Definitions.--In this section:

(1) Agency.--The term ``agency'' has the meaning given that term under section 551 of title 5, United States Code.

Just a common definition that works for this purpose.

(2) Fully functional.--The term ``fully functional'' means, with respect to a new Federal PII website, that the website can fully support the activities for which it is designed or intended with regard to the eliciting, collection, or storage of personally identifiable information, including handling a volume of queries relating to such information commensurate with the purpose for which the website is designed.

Works properly.

(3) New federal pii website.--The term ``new Federal PII website'' means a website that--

(A) is operated by (or under a contract with) an agency;

(B) elicits, collects, or stores personally identifiable information of individuals and is accessible to the public; and

(C) is first made accessible to the public and collects or stores personally identifiable information of individuals, on or after July 1, 2013.

Defines this requirement for all websites launched after July 1 2013 to avoid backlash from however many other federal websites might be out there, which are grandfathered by this definition.

(4) Operational.--The term ``operational'' means, with respect to a website, that such website elicits, collects, or stores personally identifiable information of members of the public and is accessible to the public.

Excludes test environments and the like.

(5) Personally identifiable information (pii).--The terms ``personally identifiable information'' and ``PII'' mean any information that can be associated with one individual through a social security account number, taxpayer identification number, state identification number or other identifer, but does not include information (such as name, mailing or email address, telephone number, or similar contact information) necessary to contact an individual.

An unusual definition of PII which does not include name and contact information alone, as this might make it very burdensome for agencies that need only collect basic information from people. Security only becomes very serious to require this certification when unique identifiers like SSN are collected.

(6) Responsible agency.--The term ``responsible agency'' means, with respect to a new Federal PII website, the agency that is responsible for the operation (whether directly or through contracts with other entities) of the website.

In healthcare.gov's case, this means CMS is responsible for the HHS website.

(7) Secure.--The term ``secure'' means, with respect to a

new Federal PII website, that the following requirements are met:

(A) The website has security features that meet a standard acceptable for banking purposes and the responsible agency has a named overall security leader with a comprehensive, top-down view of the security posture for the website who has supervised a complete end-to-end security test.

Should be amended to name the present standard (PCI, it is called). We were under pressure to introduce the bill for fear of another office taking the idea, as happened to us once already last year. However, please note that healthcare.gov does NOT have a named overall security leader and no end-to-end security tests were conducted.

(B) The website ensures that personally identifiable information elicited, collected, or stored in connection with the website is captured at the latest possible step in a user input sequence.

Healthcare.gov doesn't do this (for cynical political reasons).

(C) The responsible agency for the website has taken reasonable efforts to minimize domain name confusion, including through additional domain registrations and a program to educate consumers how to spot fraudulent websites.

They didn't do this.

(D) The responsible agency requires all personnel who have access to personally identifiable information in connection with the website to have completed a Standard Form 85P and signed a non-disclosure agreement with respect to personally identifiable information, and the agency takes proper precautions to ensure only trustworthy persons may access such information.

They don't do this.

(E) The responsible agency maintains (either directly or through contract) ample personnel to respond in a timely manner to issues relating to the proper functioning and security of the website, and to monitor on an ongoing basis existing and emerging security threats to the website.

They are only just now starting to do this.

(8) State.--The term ``State'' means each State of the United States, the District of Columbia, each territory or possession of the United States, and each federally recognized Indian tribe.